UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,026	10/10/2000	Marco Martins	YOR9-2000-0165	2558

48150 7590 06/07/2006

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/685,026	MARTINS ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,5-8 and 11-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-8 and 11-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3, 5-8, and 11-28 are pending in this office action, claims 4, 9, and 10 are newly canceled.

Response to Arguments

2. Applicant's arguments, filed April 17, 2006, have been fully considered and are persuasive. However, upon further consideration, a new ground(s) of rejection is made.

Claim Objections

3. Claims 5-8, 11, and 12 are objected to because of the following informalities: claims 5 and 11 are dependent upon canceled claims, the remaining claims are dependent on either claim 5 or 11. Appropriate correction is required.

Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claims 1, 3, 5-8, 11-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. (U.S. Patent No. 5,396,558) in view of Urata (U.S. Patent No. 6,799,272), and further in view of Schneier, "Applied Cryptography:

Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter Schneier).

Regarding claim 1, Ishiguro et al. teaches a method for preventing counterfeiting of a smart card, comprising:

- Providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings (fig. 4B and col. 7, lines 6-44);
    - Wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (fig. 6 and col. 10, lines 5-35);
- Providing a reader for reading said smart card including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network (fig. 9, ref. num $2M_2$ and col. 13, lines 40-43 and col. 14, lines 28-50),
    - Wherein said reader includes a random number generator (fig. 6, ref. RANDOM R and col. 13, lines 6-20), **and**
- **Periodically communicating, by said reader of said smart card, with a database where a predetermined characteristic of the card is checked** (col. 14, line 28 through col. 15, line 6).

Ishiguro et al. does not teach **wherein said smart card carries thereon predetermined N channels as C1, C2, ..., CN, where N is an integer, wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), wherein hi is the i^{th} high number and li is the i^{th} low number, and wherein said reader obtains a content of only two of said channels**, or the random number generator chooses a pair (a, b) of distinct numbers with a < b between 1 and N.

Urata teaches **wherein said smart card carries thereon predetermined N channels as C1, C2, ..., CN, where N is an integer, wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), wherein hi is the i^{th} high number and li is the i^{th} low number** (col. 2, lines 32-52 and fig. 1, ref. num 106, 128, and 142), **and wherein said reader obtains a content of only two of said channels** (col. 2, lines 37-47).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine multiple channels carrying pairs of numbers, wherein the reader obtains only two channels during a reading, as taught by Urata, with the method of Ishiguro et al. It would have been obvious for such modifications because obtaining only a limited amount of the total information on the card for a successful authentication of the card prevents people from acquiring the entire contents of the card during a single transaction (see col. 2, lines 10-29 of Urata).

The combination of Ishiguro et al. and Urata still do not teach when a card is read, choosing a pair (a, b) of distinct numbers with a < b between 1 and N.

Schneier teaches when a card is read, choosing a pair (a, b) of distinct numbers with a < b between 1 and N (a step of an RSA algorithm, choose two prime numbers, page 467).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine reading a pair of distinct numbers from the card, as taught by Schneier, with the system of Ishiguro et al./Urata. It would have been obvious for such modifications because this allows the reader to create random numbers to authenticate the smart card through challenge-response, as is commonly done in systems where a server device authenticates a client device.

Regarding claims 3 and 25, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein an entire/substantial process of said method is performable off-line (see col. 14, lines 28-31 of Ishiguro et al., this passage suggests that only occasionally will data be sent to the management center).

Regarding claim 5, applicant's admitted prior art teaches further comprising using public key cryptography with associated encoding and decoding functions Vi and Vi^{-1} in each channel i, wherein each function Vi^{-1} is known publicly, and Vi is known only to a

predetermined party representing an owner of the smart card (see page 6, lines 1-5 of applicants disclosure).

Regarding claim 6, applicant's admitted prior art teaches wherein for each i in 1, 2, ..., N, the pair (hi, Ii) is such that hi = Vi(Ii), or hi = Vi(K(Ii)), where K represents a publicly-known cryptographic hash function, and wherein each Ii contains a plurality of symbols for redundancy (see page 6, lines 6-8 of applicants disclosure).

Regarding claim 7, the combination of Ishiguro et al. as modified by Urata/Schneier teaches further comprising processing, using an invertible function f which is made public, such that the low numbers in said smart card satisfy $I(i+j) = f^j(Ii)$, where f^j represents the j^{th} iteration of the function f (see col. 5, line 48 through col. 6, line 25 of Urata).

Regarding claim 8, the combination of Ishiguro et al. as modified by Urata/Schneier teaches:

- Wherein before processing the smart card, the reader obtains the pair (ha, Ia) and hb (a step of an RSA algorithm, choose two prime numbers, see page 467 of Schneier);
- Using the public keys Va^{-1} and Vb^{-1}, checking by the reader whether the pairs (ha, Ia) and (hb, Ib) are compatible, and, consequently, that the numbers ha, Ia,

and hb belong to a same legitimate card (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 11, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein the predetermined characteristic comprises whether a smart card has delivered more than a predetermined amount of money to a user of the smart card (see col. 15, lines 36-60 of Ishiguro et al.).

Regarding claim 12, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein if a card is detected as delivering too much money, the database communicates a corresponding number I1 to all readers in a network, so that smart cards carrying said corresponding number are declined (see col. 14, lines 51-57 of Ishiguro et al.).

Regarding claim 13, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein said cryptographic structure is changed periodically (see col. 6, lines 33-42 of Urata).

Regarding claim 14, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein said smartcard is invalidated after a predetermined time of usage (see col. 16, lines 7-66 of Ishiguro et al.).

Regarding claim 15, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein said pairs (hi, li) to be contained on the smart card are generated by:

- Choosing a prefix of I1 once for all transactions, or changed whenever needed, wherein said prefix is publicly known (a step of an RSA algorithm, see page 467 of Schneier); and
- Providing a sequence, such that the sequence is generated so that a same number is not chosen twice, and so that corresponding other li's are not chosen as new I1s (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 16, the combination of Ishiguro et al. as modified by Urata/Schneier teaches further comprising:

- Concatenating the prefix and the sequence to form I1 (a step of an RSA algorithm, forming the product of two primes, see page 467 of Schneier); and
- Choosing a function f which is invertible and is publicly known, to construct I2 = f(I1), I3 f(I2), and so forth (a step of an RSA algorithm, use Euclidean algorithm on two primes, see page 467 of Schneier).

Regarding claim 17, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein the function f is chosen to be the identity map, in which case I1 = I2 = I3 = ... =IN (a step of an RSA algorithm, where the message is encrypted

in blocks, where the same encryption method is used for each block, see page 467 of Schneier).

Regarding claim 18, the combination of Ishiguro et al. as modified by Urata/Schneier teaches choosing, for a number N, N public key-private key pairs, such that a first private key V1 is for computing h1 = V1 (I1), a second private key V2 is for computing h2 = V2(I2), and so on (a step of an RSA algorithm, where the message is encrypted in blocks, see page 467 of Schneier).

Regarding claim 19, the combination of Ishiguro et al. as modified by Urata/Schneier teaches further comprising:

- Verifying whether the smart card is authentic (digital signature of an RSA algorithm, see page 473 of Schneier); and
- Checking whether the smart card is not in a list of cards to be refused (see col. 14, lines 16-23 of Ishiguro et al.).

Regarding claim 20, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein, when the smart card is read by said reader, a random generator is prompted which provides two integer numbers, a and b, which are not between 1 and N, with a < b (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 21, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein said numbers a, b are transmitted to the smart card which delivers two high numbers ha, hb, and a low number la in a channel a, and wherein the pair (a, b), together with a function f in a memory in the reader, are used to compute the low number $lb=f^{(b-a)}(la)$, said memory in said reader delivering public keys Va^{-1} and Vb^{-1} (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 22, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein the public keys are used by a comparator together with the pairs (ha, la) and (hb, lb), to verify that the pairs are compatible with the corresponding keys, and that the pairs are from a same legitimate card (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 23, the combination of Ishiguro et al. as modified by Urata/Schneier teaches further comprising performing a final validation of the smart card by at least one of:

- Contacting a central database if an entire transaction is made on-line with no penalty; and checking with a local database in said reader, said local database being refreshed periodically by contact between said local database and said central database (see col. 14, lines 16-23 of Ishiguro et al.).

Regarding claim 24, the combination of Ishiguro et al. as modified by Urata/Schneier teaches a method of preventing counterfeiting of a smart card, as explained above with the rejection of claims 1 and 8, further comprising:

- Providing a smart card such that none of confidential information and a cryptographic key for authorizing the smart card, is carried on the smart card (see col. 2, lines 32-52 of Urata);
- Reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique (see col. 2, lines 32-52 of Urata).

Regarding claim 26, the combination of Ishiguro et al. as modified by Urata/Schneier teaches a system for preventing cloning of a smart card, comprising a smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card (see col. 2, lines 32-52 of Urata).

Regarding claim 27, the combination of Ishiguro et al. as modified by Urata/Schneier teaches a computer readable medium for preventing counterfeiting and cloning of smart cards, as explained above with the rejection of claims 1 and 8, further comprising providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings (see col. 2, lines 32-52 of Urata).

Regarding claim 28, the combination of Ishiguro et al. as modified by Urata/Schneier teaches wherein information stored on said smart card is devoid of confidential information (see col. 2, lines 32-52 of Urata).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100